Special Warfare, vol. 7, nº 3, July/1994, pp. 32-39

Threat Weapons and Weapons Technologies: Implications for Army SOF

by Julie M. Merchant

There now appears to be a consensus on the national security outlook for the next decade. Undoubtedly, the post-Cold War international environment presents the United States with security challenges unprecedented in ambiguity, diversity, risk and, particularly for Army special-operations forces, opportunity. For the first time since the 1930s, no single power confronts the U.S. with a clear and present danger. However, the collapse of the Soviet empire and the end of the Cold War in many ways only exacerbate the problems facing the U.S.

For many decades, nearly all of our intelligence analysis was directed toward one country. We understood well the Soviets' strategic doctrine and tactics for conducting offensive and defensive operations and had confident estimates of the capabilities of their weapons. The Cold War environment was also one in which U.S. national security strategy carefully rationed the use of military force to only those conflicts that promoted democracy over communism. The world was a dangerous place, but the superpowers were held in check by the knowledge that each had the capability to destroy the planet.

It is not surprising that the sound of hammers tearing down the Berlin Wall was joined by voices sounding the collective ecstasy of the "new world order." Unfortunately, five years later, reality has proven that the new world order is neither new nor orderly. The old forces of adventurism, nationalism and separatism have reappeared, often with violent and unpredictable consequences. Coupled with this is a new national security strategy, still in its infancy, that allows U.S. military involvement in the complicated scenarios of operations other than war, such as peacemaking operations and nation-building efforts. The implication for Army special operations is clear: We must be continually prepared for a variety of threat forces, many with credible military capabilities due to the explosive proliferation of arms worldwide. Maintaining an awareness of weapons and weapons technologies that ARSOF may face will assist in that preparation.

Any discussion of weapons and weapons technologies must address the subject of proliferation. Proliferation, with its various implications, is the hottest defense topic of the 1990s. However, most discussions on the subject fail to define the problem specifically or to place it in perspective to the overall threat. Relevant points that must be addressed include characterization of the arms-market environment,

Author's note: This article is a condensed, unclassified version of the Army Special Operations Command briefing "Technical Threats to ARSOF." The information is derived from nonproprietary, noncopyright sources.

recognition that possession does not equal capability, and recognition of information gaps concerning proliferation to nonconventional forces. Avoiding these issues risks creating an 11-foot ghost, called proliferation, similar to the 11-foot Soviet bear created in the 1980s.

The first matter of concern is the characterization of the arms market. A decade ago the international arms market was one of many potential buyers with deep purses, but it had with very few sellers. Today, the situation has reversed. Because of fiscal constraints, arms-producing countries have resorted to massive marketing campaigns to fund research and development. Concurrently, the deep well of funds for purchasing weapons has dwindled, largely because of declining oil prices worldwide. Gone, too, are the large arms grants provided by the former Soviet Union, which aided in the buildup of countries such as Cuba and Syria. Although massive arms deals will be the exception rather than the rule, the flood of weapons on the market will allow any potential aggressor to purchase what he wants, provided he has a large-enough checkbook.

Secondly, the existence of a hostile force with an array of sophisticated weapons does not automatically present an overwhelming danger. The more important issue is whether that force also possesses the ability to fully exploit the technical capabilities of those weapons. Factors that will determine a force's ability to achieve maximum benefit from a given weapon include quality of training, professionalism of the force, ability to assimilate technology, ability to develop tactics and doctrine incorporating a heterogeneous weapons mix, and the ability to sustain and maintain a weapons inventory.

Finally, and especially important to ARSOF, most of the discussion of proliferation today involves only weapons being bought and sold by conventional standing armies. The discussion has yet to turn to perhaps the more important subject of just what is being acquired by insurgents and other paramilitary forces that ARSOF may face in future conflicts. These groups often display an unexpected creativity and flexibility in the use of low-technology weapons, thereby compounding the problems associated with assessing their capabilities.

Army special-operations forces, in the course of being deployed worldwide, may encounter forces armed with various mixes of increasingly sophisticated weaponry. It is impossible to discuss in one article the complete array of weapons that ARSOF may face. Therefore, this discussion will focus on those developments in both weapons and weapons technologies that will have the greatest implications for ARSOF operations now and in the future.

Reconnaissance

Reconnaissance, surveillance and target acquisition, or RSTA, continues to be one of the most important combat-support functions on the modern battlefield. Timely, accurate intelligence on the disposition and location of enemy forces is prerequisite to the success of any operation. The current international arms market offers a myriad of systems and technologies that enhance both man- and machine-operational RSTA capabilities. These systems and technologies, which include electro-optical sensors, acoustic/seismic sensors and reconnaissance platforms, are used with varying degrees of success in many regions worldwide.

Many nations are purchasing surveillance and reconnaissance systems primarily for employment in a defensive, early-warning and intelligence- acquisition mode. While the majority of such systems provide a long-range, daylight-surveillance capability, they also enhance soldiers' nighttime fighting abilities. Of all the technological advances occurring in this field, the development and proliferation of electro-optical devices, along with "real time" automated processing of data received from existing sensors, will have the greatest implications for special-operations forces.

U.S. night doctrine and the corresponding reliance on EO sensors such as night-vision devices were widely reported during the conflict in the Gulf and, more recently, in Somalia. EO sensors include infrared

U.S. Army photo

A soldier uses a hand-held infrared surveillance device.

image converters, image intensifiers, thermal imagers and low-light-level televisions. U.S. industrial-manufacturing capabilities in this area are unsurpassed; however, widespread awareness of U.S. capabilities has caused rampant growth in the development and acquisition of vision-enhancement devices worldwide. The proliferation of these systems has obvious implications for operations conducted under the cloak of darkness. Integrating EO technology with weapons such as man-portable surface-to-air missiles will mean that concealment of darkness can no longer be assured for SOF aviation units.

The first generation of EO devices came in the form of infrared image convertors fielded by Germany during the last years of World War II. Still in use, these systems employ infrared illumination devices, such as searchlights, with the visible light filtered out. With a target-recognition range of about 1.5 km, infrared night-vision devices allow troops to operate at night without being seen, unless the opposing force has similar systems. Infrared convertors are still being installed on eastern European and Asian vehicles despite their obsolescence in the West, and the potential for their removal and subsequent use as independent systems is great.

Image intensifiers represent the next level of EO sensor development. These systems, incorporating increasingly sensitive photo-cathode material that allows them to operate with natural nighttime ambient light, were introduced into military inventories in the 1960s. Successive generations of systems have produced intensifiers with increased sensitivities, higher resolutions and longer battery life.

U.S. industry is currently enhancing the production of third-generation devices and leads the way in the development and production of fourth-generation image-intensifier devices. While manufacturers espouse the benefits of third-generation devices (three times the sensitivity, twice the image resolution, and about three times the battery life of second-generation systems), few have reached the international arms market. Second-generation systems will be widely sought by forces which need a reliable night-operation capability. Third-generation systems most likely will be available only to countries or organizations willing to spend larger amounts of money for the increased capabilities.

The development of image-intensifier devices was followed by the development of thermal-imaging systems, which require no illumination and operate on thermal emissions from objects in the field of view. Different target aspects may be revealed by the system's ability to move the polarity of the image between white/hot to black/hot. Another advantage of thermal-imaging systems is that they may be used during daytime operations to "see" through external camouflage and battlefield smoke, thereby revealing potential targets. First-generation TI systems are available worldwide and will be used increasingly throughout the remainder of the century. Future generations of these devices, including man-portable systems, will escalate in importance as manufacturing capabilities spread and systems become available on the international market.

Finally, low-light-level television devices integrate image-intensifier systems and TV systems, resulting in an image display or processing at low ambient-light levels.

Coupling a second- or third-generation image-intensifier tube to a TV camera — technology that can be acquired at an electronics shop — produces a solid-state, rugged, low-light-level TV camera. LLLTV systems are being incorporated into other military systems, such as vehicles and weapons, as less expensive alternatives to thermal-imaging devices. Because of their low cost, LLLTVs are affordable systems for forces that can purchase off-the-shelf equipment and modify it for military use.

Automation of resources supporting RSTA is an additional area in which the return on investments will be great. Forces with insufficient automated-data-processing capabilities will not be able to perform real-time processing of the data received by the myriad of RSTA sensors and platforms already built and fielded. To this end, military organizations may invest varying amounts of money to achieve equitable capabilities, depending on the range of their operations. Small paramilitary forces may integrate laptop computers with existing sensors to improve perimeter security, while nations recognizing the importance of the knowledge-based battlefield may establish powerful and expensive automated-data-processing resources to reap the benefits of expensive RSTA sensors and systems across the battlefield.

Electronic warfare

Effective radio communications are a fundamental requirement for mobile operations, yet they can easily become the target of electronic-warfare measures such as jamming, geolocation and interception. EW contributes to the disruption of command and control at decisive points and is a key element on the battlefield. Although EW techniques may be used on all types of electronic systems, of major concern to ARSOF are the technologies that aim to intercept, geolocate or jam communications; and the use of EW against ARSOF information systems.

The extent to which EW systems have been manufactured and fielded has been well-established by open-source publications. A review of these sources reveals that a variety of systems covering the entire electromagnetic frequency spectrum is available worldwide. Ranging from sophisticated airborne platforms to simple, remotely delivered ground systems, these systems will enable hostile forces to use a variety of communication-jamming techniques and to locate and intercept signals. For most forces, the advancements in these systems and their proliferation lessen the challenge of countering unencrypted narrow-band communications. As communications begin to use modern modulation schemes such as direct sequence, frequency hopping or hybrid spreading, EW equipment designed to counter these modulations will emerge. Spaced-based communications are also likely to be increasingly targeted as forces worldwide begin to rely more heavily on satellites as relays.

The capabilities to engage in EW may vary greatly. While the latest technology is available on the open market, forces that have not invested heavily in sophisticated systems may not be able to cover the entire frequency spectrum using automatically tuned systems. To communicate without interference or detection, ARSOF must understand the EW systems available to the opposing force.

Computers, computer systems and automated networks are pervasive in the Department of Defense. Critical to the support of ARSOF operations across the tactical, strategic and sustaining-base environments, these systems make attractive targets. The threat is genuine and is growing. Potential adversaries are individuals or groups, both foreign and domestic, who have the capability and the intent to exploit a system. Their motives include military, political or industrial gain as well as personal amusement.

Adversaries have three primary objectives: the compromise of information, the corruption of data and the disruption of operations. To achieve their objectives, they may use an individual equipped with a personal computer, modem and telephone line; or they may use multiple actors and governmental support. The likelihood of a given threat varies depending on whether the information system is

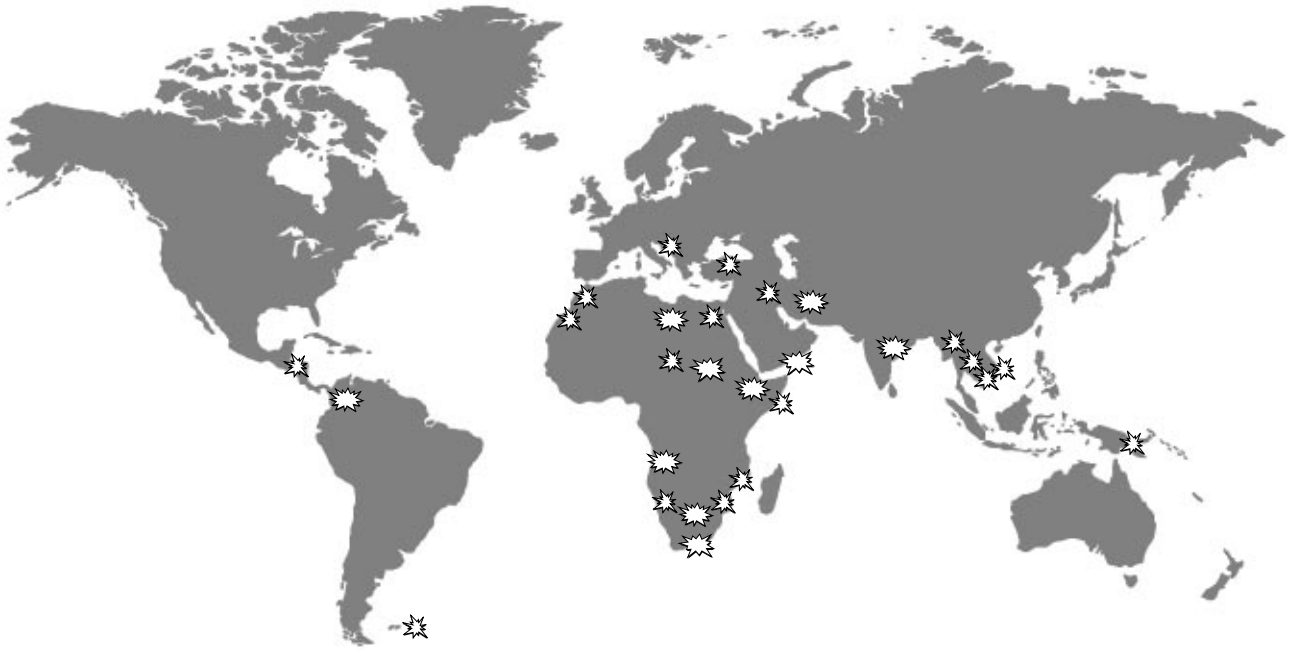
deployed in the tactical, strategic or sustaining-base environment.

A case demonstrating the threat to information systems is that of the Hannover Hackers. From the mid- to late 1980s, a group of German computer hackers from West Berlin and Hannover used the German telephone network to enter computers at the universities of Karlsruhe and Bremen. From there they connected to international telephone networks and gained access to computers in the U.S., Canada, Japan and western Europe. According to some reports, the hackers were successful in more than 40 percent of their remote log-in attempts. To enter the systems they relied on purchased, stolen or copied passwords, the testing of likely passwords, and the random generation of passwords. Upon log-in, the hackers granted themselves privileges and then installed a Trojan horse that allowed them to record authorized passwords from unknowing users.

Mines

A rapid evolution has taken place in mine technology over the last two decades, and an increased emphasis on mine warfare throughout the world has created an expanding market for all types of mine systems. Their low cost, indefinite shelf life and manpower savings explain their wide appeal. Land and naval mines are now essential weapons in conflicts at all levels: from grass-roots insurgencies to major confrontations between well-equipped armies. Effective mine warfare obstructs the mobility of opposing forces and creates favorable conditions for the

Countries With Significant Landmine Incidents



Honduras	Botswana	Western Sahara	Iraq	India
Nicaragua	Namibia	Morocco	Iran	Burma
Costa Rica	Angola	Libya	The Yemens	Thailand
Colombia	Former Yugoslavia	Egypt	Somalia	Cambodia
Falkland Islands	Sudan	Turkey	Mozambique	Vietnam
South Africa	Chad	Ethiopia	Zimbabwe	New Guinea

mine employer.

Modern mines were first used on the battlefield near the end of World War I in response to the emergence of the tank. Mines evolved into a serious threat during World War II when conventional anti-tank mines and anti-personnel fragmentation mines were widely used. Today, an estimated 85-100 million anti-personnel and anti-vehicle mines may lie unexploded in more than 60 nations. Countries with the highest density of mine employment include Afghanistan, Angola, Somalia and Cambodia, where civil-war combatants used the explosive devices to terrorize civilian populations. Mines pose problems long after conflicts; they can be a definite deterrent to light industry, agriculture, repatriation of refugees and overall nation-building processes in which ARSOF may be involved.

Evolving technology is making mines more deadly, more disruptive and more economical. Developments in areas such as remote delivery, detectability, blast-resistant fusing, multiple sensors and "smart" systems have boosted the effectiveness of current systems. They have also simplified laying of the fields and have lowered logistical burdens. The percentage of advanced-technology mines is increasing; and even though new technology is costly, mines are still affordable weapons for any military organization.

The surge of technological sophistication in mines presents keen challenges to the U.S. countermine-development program. Foreign mines are developed with a fair understanding of countermine concepts and are designed to counter detection, identification, removal, neutralization and predetonation. Developmental lead time for mines is much shorter than for countermine programs. Any country can purchase mines to counter specific countermine capabilities or developments.

Air defense

Desert Storm demonstrated the role that air forces can play in preparing the way for ground attacks. Recognizing the importance of air assets, threat forces will seek the most effective weapons to deny air superiority, whether on a limited scale, as in Somalia, or on a greater scale, as in major regional conflicts. Currently, surface-to-air missile systems are the foremost choice.

Surface-to-air missiles can be divided into two categories: those that use radio-frequencies to guide and track the missile through flight, and those that use infrared guidance to target thermal emissions of aircraft. Infrared systems are usually man-portable. Over the last several years, an incredible amount of information has surfaced on surface-to-air systems engineered and manufactured by countries around the world, especially systems offered for sale by Russia. The capabilities of these systems, spanning tactical and strategic ranges, have been widely advertised at trade shows, which indicates their availability on the arms market. Prices range from several million dollars for sophisticated RF systems to several thousand for infrared systems.

U.S. Army photo

A soldier practices the use of an SA-7 surface-to-air missile.

The publicized effectiveness of the Stinger in Afghanistan and both the SA-7 and the SA-14 in El Salvador, along with their relatively low cost, has caused man-portable systems to be widely sought. Because of their ease of employment, these systems have the potential to disrupt ARSOF missions. Originally, visual

target acquisition made man-portable systems nearly ineffective at night. As previously mentioned, however, their combination with night-vision devices could give threat forces a credible nighttime air-defense capability.

Unmanned aerial vehicles have existed since the 1930s and have been used in combat by many nations. Although they have been widely used by Israel during the last two decades, it was not until Desert Storm that the full value of UAVs as inexpensive airborne platforms was realized. Most UAVs now in development use strap-on payloads and are intended for multimission purposes. This feature provides an inexpensive and flexible capability for reconnaissance, communications, electronic warfare or direct attack. The cost of a typical multimission UAV, including payloads, is 0.1 to 1 percent of the cost of a typical manned aircraft and thus may be affordable for even the smallest of potential adversaries, especially those who choose off-the-shelf systems and modify them for a specific use.

Directed energy

Conventional small-arms technology is rapidly nearing its limit worldwide. Weapons will reach their limits of precision within 10-15 years. As industry looks to the future, it will probably pursue technologies using "energy bullets" fired from directed-energy weapons.

Directed-energy weapons, including lasers, radio-frequency weapons and particle-beam weapons, have several advantages over more conventional weapons systems. One advantage is their nearly instantaneous flight to target. Thus, the potential for retargeting is considerable, allowing for the engagement of a multitude of targets over a wide field of view. Targets can also be engaged at reduced ranges, where the probability of target hard kill is increased. A disadvantage of DEWs is weapon performance may be hindered by inclement weather.

The most likely developments of the next decade will be in laser technologies. Increasingly prevalent on the modern battlefield, lasers are used in range determination, target designation, target guidance and communication. Long postulated as a means of surpassing the sophisticated weapons of the modern battlefield, laser weapons have shed their futuristic image and are now a modern reality.

Laser weapons can be divided into two

U.S. Army photo

A soldier wears a Soviet-made protective suit against nuclear, biological and chemical hazards. The NBC threat is likely to continue as nations export their stocks to other countries.

categories: low-energy and high-energy. Low-energy laser weapons attack the sensors on military equipment and the eyes of personnel. Their application produces a "soft kill," which eliminates or interferes with only a specialized function of the target, such as sight. High-energy laser weapons can attack the same range of targets, producing soft-kills at greater ranges or "hard kills," which structurally damage the targets.

Any country or organization with a modest engineering capability can adapt certain commercially available lasers for use in a limited role as blinding weapons. Current Western export controls are not sufficient to control the proliferation of weapon-quality lasers. Countries outside Western export control may also be eager to sell laser equipment. The increasing availability of laser hardware and new technology make the development of "low technology" weapons a real possibility.

Weapons of mass destruction include nuclear, biological and chemical weapons. In the last several years, the international community has expressed growing concern regarding these weapons. WMD in the hands of hostile forces threaten not only U.S. lives but also the viability of our regional power-projection strategy. Attempts to control the export of these weapons and their associated technologies have been unsuccessful, and proliferation is likely to continue until we can enforce export controls. Until then, ARSOF must be prepared to operate, survive and accomplish their missions in nuclear, biological and chemical environments.

No single dominating threat, such as the former Soviet Union, will be the undisputed focus of U.S. security policy during the next decade. Many smaller powers (Third World countries as well as paramilitary forces) are acquiring increasingly powerful and diverse military capabilities, thereby narrowing the technology gap that now favors the U.S. Regional powers will continue their military buildup as a result of transfers of high-technology hardware from major arms exporters and an expansion of indigenous production capabilities.

Besides the products of the major exporters — the U.S., Russia, China and certain European countries — those of other countries such as Argentina, Brazil, North Korea, Pakistan and South Africa will add to market supplies. Overall, continuing improvements in weapons systems and military capabilities and the availability of these improvements to any hostile force will increasingly threaten ARSOF's ability to enter an area either overtly or clandestinely, sustain long-term operations, accomplish specific missions, report information and intelligence to higher authorities and extract forces without discovery.

Julie M. Merchant currently serves as the scientific and technical intelligence analyst in the Office of the Deputy Chief of Staff, U.S. Army Special Operations Command. Prior to this assignment, she served as a threat analyst for the U.S. Army Missile Command, Huntsville, Ala., and as the special-projects officer with the U.S. Army Support Group-Forward in Saudi Arabia. She is a graduate of the State University of New York at Oneonta and is currently completing a master's degree in engineering from the University of Alabama at Huntsville.